BY ORDER OF THE COMMANDER,
PACIFIC AIR FORCES

PACAF PAMPHLET 31-2

19 FEBRUARY 1999

Security

INVESTIGATIONS OF ACTUAL OR POTENTIAL COMPROMISE OF CLASSIFIED INFORMATION

OPR: HQ PACAF/SFI
(SMSgt Randy N. Akers)

Certified by: (HQ PACAF/SFI
(Mr. Berry B. Rigdon)
Pages: 14
Distribution: F

This pamphlet will assist unit security managers, appointing authorities, and investigating officials to better understand and effectively manage security investigations to determine if an actual or potential compromise of classified information occurred. This pamphlet is a good tool for conducting training with people that handle classified information. The pamphlet also contains checklists to assist persons involved with the investigative process. Guidance offered by this pamphlet is suggested, not directive in nature. This pamphlet does not apply to Air National Guard or Air Force Reserve forces.

1. Terms. These terms provide unit security managers, appointing officials, and investigating officials a better understanding of the investigation process.

1.1. Access: the ability and opportunity to obtain knowledge of classified information.

1.2. Appointing Authority: MAJCOM Directorates, Numbered Air Force Staff Agency Chiefs, wing, group, squadron and detachment commanders.

1.3. Classification Guide: A document issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each element.

1.4. Compromise: an unauthorized disclosure of classified information.

1.5. Derivative Classification: The process of determining whether information has already been originally classified and, if it has, ensuring that it continues to be identified as classified by marking in newly created material.

1.6. Information Security Program Manager (ISPM): the senior security forces official at each command or installation that manages the activity or installation's information security program.

1.7. Infraction: any knowing, willful, or negligent action that does not comprise a violation. For example: an individual leaves a safe insecure, locks all doors and windows, and goes home for the

evening. If the investigating official determines no unauthorized access was gained into the room, this would be an infraction, since classified information was not compromised.

1.8. Investigating Official: any commissioned officer, senior noncommissioned officer, or civil service employee equivalent to a senior noncommissioned officer, and designated by an appointing authority to conduct an investigation.

1.9. Investigation: an authorized, systematic, detailed examination to uncover the facts and determine the truth of a matter.

1.10. Original Classification Authority: an individual that makes an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

1.11. Unauthorized Disclosure: a communication or physical transfer of classified information to an unauthorized recipient.

1.12. Violation: any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information, or any action to classify information or continue to classify information that violates directives.

2. Policy. See DoD 5200.1-R, *Information Security Program*, and AFI 31-401, *Managing the Information Security Program*, for policy related to actual or potential compromise of classified information.

3. Responsibilities.

3.1. Individual. Anyone finding insecure classified material or who becomes aware of the possible compromise of classified information shall:

3.1.1. Take custody of and safeguard the material.

3.1.2. Immediately report it to their supervisor, unit security manager, or commander. If any of these people are involved, report to the next person in the chain of command.

3.1.3. Treat the notification at the same level of classification as the information involved whenever the information is accessible to unauthorized personnel.

3.1.4. If classified information appears in the public media, do not make any statement that would confirm the accuracy or verify the classified status of the information. If approached by media persons, do not confirm or deny the accuracy of the classification of the information and immediately report the situation to a supervisor, unit security manager, or commander.

3.2. Unit Security Managers. The unit security manager has many responsibilities and is normally the person that gets the ball rolling in the investigation process. The unit security manager's involvement starts when notified of the incident, and is not complete until the report is finalized. As a minimum, the unit security manager must:

3.2.1. Ensure appropriate measures are taken to regain custody of the document or material.

3.2.2. Take measures to negate or minimize the adverse effect of an actual or potential compromise of classified information.

3.2.3. Ensure notifications are classified at the same level as the information involved until the information is retrieved and appropriate safeguards are in place.

3.2.4. Notify the ISPM of the situation within 24 hours of the incident and obtain a control number.

3.2.5. Notify the appointing authority of the situation and the need to appoint an investigating official.

3.2.6. Ensure the appointment letter is accomplished for the appointing authority.

3.2.7. Provide the investigating official with all available details of the situation, and actions taken to recover and safeguard the classified information.

3.2.8. Instruct the investigating official to report to the ISPM for a briefing.

3.2.9. Monitor the status of the investigation and keep the ISPM informed whenever extensions are granted.

3.2.10. File a copy of the report IAW AFI 37-139.

3.2.11. Implement procedures in operating instructions and provide training to prevent recurrence of incidents.

3.3. Commander. Wing, Group, Squadron, and Detachment Commanders, and Directors at HQ PACAF and Numbered Air Forces, may serve as appointing authorities and bear the responsibility of administering the investigation process to ensure U.S. interests are protected. As the appointing authority the commander or director appoints investigating officials, closes reports and makes comments, and ensures prompt and appropriate sanctions are imposed on those people that knowingly, willfully, or negligently violate DoD and Air Force Information Security Programs. This pamphlet will discuss only the appointment of investigating officials and report review processes.

3.3.1. Appointing an Investigating Official. The PACAF standard is to appoint the investigating official by the end of the duty day following discovery. The unit security manager should not be appointed. Investigating officials:

3.3.1.1. Are always designated in writing (see **Attachment 1**).

3.3.1.2. Must have a security clearance equal to the classification of material involved.

3.3.1.3. Must be appointed to prevent allegations of biased reporting.

3.3.1.3.1. Do not appoint a person directly or indirectly involved in the incident.

3.3.1.3.2. Should be higher in grade than the person(s) involved in the incident.

3.3.1.3.3. Should be from an outside unit only when it is believed an unbiased investigation could not be conducted due to the nature of the incident and the persons involved.

3.3.1.4. Investigating officials are authorized up to 30 duty days from date of appointment to complete the investigation. This period may be shortened. Extensions may be granted in unusual circumstances.

3.3.2. Closing Reports. Commanders and directors approve and close reports. Reports will be unclassified except in extreme circumstances.

3.4. Investigating Official. This is the key person in the investigation process. In general, the investigating official is responsible for determining whether classified information was compromised. The highest priority for the investigating official is to determine if the custody of the classified infor-

mation in question has been regained and that proper safeguarding measures have been taken to negate or minimize the adverse effect of a compromise. When this has been accomplished the investigating official can then determine if an actual or potential compromise occurred. To reach this conclusion there are several actions the investigating official should take.

3.4.1. Conducting the Investigation.

3.4.1.1. The investigation should be completed prior to the suspense established by the Appointing Authority. Only the Appointing Authority may grant extensions.

3.4.1.2. Immediately after appointment, contact unit security manager and determine the circumstances of the incident.

3.4.1.3. Contact the ISPM and receive a briefing.

3.4.1.4. Contact the local staff judge advocate to have all legal questions answered.

3.4.1.5. Determine if custody of the classified information has been regained.

3.4.1.6. Determine the measures that have been taken to negate and minimize the effects of a compromise. For example: have local area networks on the sending and receiving ends been shut down and scrubbed.

3.4.1.7. Obtain a copy of the appointment letter.

3.4.1.8. Determine if the classified information in question was properly classified.

3.4.1.9. Determine when, where, and how the incident occurred. This may require personal interviews. If a personal interview is conducted, get the interview in writing.

3.4.1.10. Based upon the facts, determine if a compromise occurred.

3.4.1.11. If compromise occurred:

3.4.1.11.1. Immediately notify the originating activity. If the activity no longer exists, determine the activity that inherited the functions of the originating activity. If this cannot be determined, or the functions of the originating activity have been dispersed to more than one activity, notify the Office of the Secretary of the Air Force. **NOTE: Do not delay this notification to complete the investigation or resolve other related issues**.

3.4.1.11.2. If possible, determine to what extent the information was disseminated.

3.4.1.11.3. If the classified information was compromised to the media, determine in what specific article or program it appeared.

3.4.1.11.4. If the compromise is due to a loss of classified information, determine what steps were taken to locate the material.

3.4.1.11.5. Determine if a weakness or vulnerability exists in security practices or procedures that led to the compromise.

3.4.1.11.6. Determine if the compromise was due to a failure of a person(s) to comply with established security practices or procedures.

3.4.1.11.7. Identify all persons that had unauthorized access to classified information and debrief these people.

3.4.1.11.7.1. Annotate the debriefing on AF Form 2587. All persons debriefed are required to sign the form. If the person refuses to sign the form, annotate the refusal and any reasons given for the refusal, and include in the report.

3.4.1.11.7.2. If the person has an appropriate security clearance but no need-to-know, ensure the person is aware that the information is classified and requires protection.

3.4.1.11.7.3. If the person does not possess an appropriate security clearance, and is a U.S. Government civilian, military person or an employee of a cleared U.S. Government contractor, advise the person of their responsibility to prevent further dissemination of the information and administrative sanctions and criminal penalties for failure to do so. Design this briefing to educate the person on what classified information is, the importance to protect it, and what to do if someone tries to obtain it. Notify the person's parent organization when this occurs.

3.4.1.11.7.4. If the person is not a member of an U.S. Government organization, or an employee of a cleared contractor, consult with the staff judge advocate before attempting to debrief the individual.

3.4.1.12. If compromise **did not** occur:

3.4.1.12.1. Determine if the infraction occurred due to failure to comply with established security practices or procedures.

3.4.1.12.2. Determine if there is a weakness or vulnerability in established security practices or procedures that could lead to a compromise if not corrected.

3.4.2. Completing the Report. Document the results of the investigation (see **Attachment 2**).

3.4.2.1. All reports should address:

3.4.2.1.1. Whether the information was properly classified.

3.4.2.1.2. The specific information involved.

3.4.2.1.3. The when, where, and how the incident occurred.

3.4.2.1.4. What persons, situations, or conditions caused or contributed to the incident.

3.4.2.1.5. The steps taken to locate lost classified information.

3.4.2.1.6. Whether a compromise did or did not occur.

3.4.2.1.7. The corrective actions taken to prevent further recurrence.

3.4.2.2. If a compromise occurred, in addition to the above areas in 3.4.2.1, the report needs to address:

3.4.2.2.1. To what extent was the compromised information disseminated.

3.4.2.2.2. That the originator of the information was contacted.

3.4.2.2.3. The identify of the specific article or program if compromised to the public media.

3.4.2.2.4. The names of the persons that required debriefing.

3.4.2.3. Submit the report to the ISPM for review. This will prevent processing delays.

3.4.2.4. After ISPM review, submit the report to the Appointing Authority.

3.4.2.5. Once approved, provide the original to the unit security manager and a copy to the ISPM.

DOSS C. VON BRANDENSTEIN, Col, USAF
Director, Security Forces

Attachment 1

SAMPLE APPOINTMENT LETTER

MEMORANDUM FOR (INVESTIGATING OFFICIAL)

FROM: (APPOINTING AUTHORITY)

SUBJECT: Appointment of Investigating Official

References: (a) DoD 5200.1-R, *Information Security Program*

(b) AFI 31-401, *Managing the Information Security Program*

1. You are tasked with conducting an investigation into a suspected compromise of classified information. Keep a copy of this letter on your person throughout the investigation. Conducting the investigation will be your primary duty until it is completed. The purpose of this investigation is to determine:

a. Whether the information was properly classified.

b. The when, where, and how the incident occurred.

c. What persons, situations, or conditions caused or contributed to the incident.

d. The steps taken to locate lost classified information.

e. Whether a compromise did or did not occur. If a compromise occured, contact me immediately and provide the below information:

(1) To what extent was the compromised information disseminated.

(2) The name or office of the originator of the information.

(3) The specific article or program if compromised to the public media.

f. The corrective actions that will prevent further recurrence.

2. Prior to initiating this investigation contact the following people:

a. Unit security manager: receive a full briefing on the incident.

b. Installation Security Program Manager (ISPM): this is the security force's information security specialist.

c. Staff Judge Advocate: to answer any legal questions.

3. You are authorized to interview those persons necessary to complete your investigation. You are authorized access to all records and files to include classified information at the (identify investigating officials security clearance, i.e. top secret, secret, SCI) level that pertains to this investigation.

4. Use the format in PACAF Pamphlet 31-2 to complete your report. Before submitting the report to me, have it reviewed by the ISPM for technical accuracy. Your suspense is (not to exceed 30 working days). Should you require an extension please contact me. If an extension is granted you are responsible for notifying the unit security manager and the ISPM.

Appointing Authority Signature Block

Attachment 2

SAMPLE REPORT FORMAT

MEMORANDUM FOR (APPOINTING AUTHORITY)

FROM: (INVESTIGATING OFFICIAL DUTY SECTION)

SUBJECT: Security Investigation # (NUMBER ASSIGNED BY ISPM)

1. AUTHORITY. An investigation was conducted to determine if classified information had been compromised IAW the attached appointing authority letter.

2. PEOPLE INTERVIEWED. Names, ranks, duty titles, and office symbols of all people interviewed.

3. FACTS. List chronologically, from the time the incident was discovered, all facts pertaining to the incident. Do not state opinion or make assumptions. The section must cover the who, what, where, when, why, and how. Keep in mind a priority system:

a. Was custody of the information regained?

b. What persons, situations, or conditions caused or contributed to the incident.

4. CONCLUSION. This section requires the investigating official to make a decision, based on the facts, as to whether a compromise occurred or did not occur.

a. The first sentence must state one of the following: **Note**: If a person is given unauthorized access or information is transmitted by unsecure means, such as local area networks, insecure fax, or insecure telephone, a violation has occurred and the investigating official must use either statement (1) or (2) below.

(1) A violation occurred and classified information was compromised. Damage to national security suspected. Original Classification Authority notified.

(2) A violation occurred and a potential compromise of classified information occurred, however, damage to national security is not suspected.

(3) An infraction occurred that could lead to potential compromise of classified information due to person(s) failure to comply with established procedures.

(4) An infraction occurred that could lead to a potential compromise of classified information due to a weakness or vulnerability in established security practices and procedures.

b. The second sentence must state one of the following:

(1) This incident caused unauthorized access. **NOTE**: Unauthorized access results from: improper marking, unauthorized transmission, improper storage, unauthorized reproduction, improper classification, or improper destruction. List one or more of these reasons that contributed to the unauthorized access)

(2) This incident resulted from improper marking.

(3) This incident resulted from unauthorized transmission.

(4) This incident resulted from improper storage.

(5) This incident resulted from unauthorized reproduction.

(6) This incident resulted from improper classification.

(7) This incident resulted from improper destruction.

(8) This incident resulted from (identify other reason if not listed in (1) - (7) above).

4. The following person(s) was debriefed **(only if required)**.

5. RECOMMENDATION. Identify solution(s) that will prevent recurrence.

6. CLOSING. The Information Security Program Manager reviewed this report. If there are any questions please contact me at 449-1234.

INVESTIGATING OFFICIALS SIGNATURE

1st Indorsement

FROM: (APPOINTING AUTHORITY)

I have reviewed this report and concur with the results. NOTE: Appointing Authority may provide additional comments as needed.

APPOINTING AUTHORITY'S SIGNATURE

Attachment 3

UNIT SECURITY MANAGER CHECKLIST

A3.1. Ensure appropriate measures are taken to regain custody of the document or material.

A3.2. Take measures to negate or minimize the adverse effect of an actual or potential compromise of classified information.

A3.3. Ensure notifications are classified at the same level as the information involved, until the information is retrieved and appropriate safeguards are in place.

A3.4. Notify the Installation Security Program Manager (ISPM) of the situation by the end of the first duty day.

A3.5. Notify the appointing authority of the situation and the need to appoint an investigating official.

A3.6. Submit the appointment letter to the ISPM (by end of duty day is PACAF standard).

A3.7. Provide the investigating official with details of the situation, and actions taken to recover and safeguard the classified information.

A3.8. Instruct the investigating official to report to the ISPM for a briefing.

A3.9. Monitor the status of the investigation and keep the ISPM informed whenever extensions are granted.

A3.10. Review investigating official comments, and implement procedures or provide training to prevent recurrence of incidents

A3.11. File a copy of the report IAW AFI 37-139.

Attachment 4

APPOINTING OFFICIAL CHECKLIST

A4.1. Selecting an Investigating Official. Use the below criteria to assist with this process.

A4.1.1. Does the situation warrant appointing an investigating official from outside the unit due to the nature of the incident or the people involved? If so consider the below options for selecting an investigating official:

A4.1.1.1. Elevate the situation to the next level of command.

A4.1.1.2. Work laterally with another commander or director to appoint the official.

A4.1.2. Select a commissioned officer, senior noncommissioned officer, or civil service employee equivalent to a senior noncommissioned officer, that is equal to or higher in rank than the person(s) involved.

A4.1.2.1. Does the person have a security clearance equal to the classification of material involved?

A4.1.2.2. Is the person in a position that prevents allegations of biased reporting?

A4.1.2.3. Is the person involved in the incident?

A4.1.2.4. Can the person be relieved of all assigned duties until the investigation is completed?

A4.1.2.5. Does the person have the ability to conduct an effective investigation?

A4.2. Appoint the Investigating Official.

A4.2.1. Designate the person in writing (see **Attachment 1** for sample letter).

A4.2.2. Submit the appointment letter to the Installation Security Program Manager (ISPM).

A4.2.3. When necessary, grant extensions in writing. Forward the extension letter to the ISPM.

A4.3. Close the report. Indorse the report and take actions deemed necessary.

Attachment 5

INVESTIGATING OFFICIAL CHECKLIST

A5.1. Get Ready to Investigate.

A5.1.1. Obtain a copy of the appointment letter as soon as it is published.

A5.1.2. Complete the investigation within the suspense. Contact the appointing authority to request extensions.

A5.1.3. Contact unit security manager and determine the circumstances of the incident.

A5.1.4. Contact the Installation Security Program Manager and receive a briefing.

A5.1.5. Contact the local staff judge advocate to have all legal questions answered.

A5.1.6. If the information is accessible to unauthorized persons, all notifications concerning the incident are classified at the same level as the information involved.

A5.2. Investigate.

A5.2.1. Determine if custody of the classified information in question has been regained.

A5.2.2. Determine if proper safeguard measures have been taken to negate or minimize the adverse effect of a compromise.

A5.2.3. Determine if the classified information in question was properly classified.

A5.2.4. Determine when, where, and how the incident occurred. This may require personal interviews. If a personal interview is conducted, get the interview in writing.

A5.2.5. Based upon the facts, determine if a compromise occurred. If compromise occurred:

A5.2.5.1. Immediately notify the originating activity. If the activity no longer exists, determine the activity that inherited the functions of the originating activity. If this cannot be determined, or the functions of the originating activity have been dispersed to more than one activity, notify the Office of the Secretary of the Air Force. NOTE: do not delay this notification to complete the investigation or resolve other related issues.

A5.2.5.2. Determine to what extent the information was disseminated.

A5.2.5.3. If the classified information was compromised to the media, determine in what article or program it appeared.

A5.2.5.4. If classified information is lost, determine what steps were taken to locate the material.

A5.2.5.5. Determine if a weakness or vulnerability exists in security practices or procedures that led to the compromise.

A5.2.5.6. Determine if the compromise was due to a failure of a person(s) to comply with established security practices or procedures.

A5.2.5.7. Determine if the compromise was due to a failure of a person(s) to comply with established security practices or procedures.

A5.2.5.8. Identify all persons that had unauthorized access to classified information. Debrief these people (see step A5.3).

A5.2.6. If compromise did not occur:

A5.2.6.1. Determine if there is potential for compromise of classified information due to failure of person(s) to comply with established security practices or procedures.

A5.2.6.2. Determine if there is a weakness or vulnerability in established security practices or procedures that could lead to a compromise if not corrected.

A5.3. Debriefings.

A5.3.1. Annotate debriefing on AF Form 2587. If the person refuses to sign the form, annotate the specific reasons for the refusal in the report.

A5.3.2. Debrief according to the situation. There are three situations that may occur:

A5.3.2.1. Person with appropriate security clearance but no need-to-know.

A5.3.2.1.1. Ensure the person is aware that the information is classified.

A5.3.2.1.2. Inform the person on protection requirements.

A5.3.2.2. Person does not have a security clearance, but is in the military, a U.S. Government civilian, or employee of a cleared U.S. Government contractor.

A5.3.2.2.1. Advise the person of their responsibility to prevent further dissemination of the information.

A5.3.2.2.2. Advise the person of the administrative sanctions and criminal penalties for failure to do so.

A5.3.2.2.3. Design this briefing to educate the person on what classified information is, the importance to protect it, and what to do if someone tries to obtain it.

A5.3.2.2.4. Notify the person's parent organization when this occurs.

A5.3.2.3. If the person does not possess a security clearance, and is not a military member, member of a U.S. Government organization, or an employee of a cleared U.S. Government contractor, consult with the staff judge advocate on how to proceed.

A5.4. Complete the Report. Document the results of the investigation (see **Attachment 2**).

A5.4.1. Keep reports unclassified **except** in extreme circumstances.

A5.4.2. Address the following areas:

A5.4.2.1. Whether the information was properly classified.

A5.4.2.2. The specific information involved.

A5.4.2.3. The when, where, and how the incident occurred.

A5.4.2.4. What persons, situations, or conditions caused or contributed to the incident.

A5.4.2.5. The steps taken to locate loss classified information.

A5.4.2.6. Whether a compromise did or did not occur.

A5.4.2.6.1. To what extent was the compromised information disseminated?

A5.4.2.6.2. Is the specific article or program identified if compromised to the public media?

A5.4.2.6.3. Was the originator of the information contacted?

A5.4.2.7. The corrective actions taken to prevent further recurrence.

A5.4.2.8. The results of debriefings.

A5.4.3. Submit the report to the ISPM for review.

A5.4.4. After ISPM review, submit the report to the Appointing Authority.

A5.4.5. After approval by Appointing Authority, provide the original to the unit security manager and a copy to the ISPM.